Cloud computing Privacy and Security

Ms. Shilpa Das
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112
Email Id: d.shilpa@jainuniversity.ac.in

Abstract

A big concern in information technology has consistently been data protection. It is especially serious in the cloud computing setting because the data is stored in various locations, even across the globe. The two key reasons for consumer concerns about cloud technology are data security and privacy protection. Although many techniques have been investigated in both academia and industries on cloud computing topics, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. In the cloud architecture, data security and privacy protection problems are relevant to both hardware and software. This study explores various security approaches and challenges for data protection in the cloud, from both software and hardware perspectives, and aims to enhance data security and privacy protection for the trusted cloud environment. In this paper, we compare the current research work on data security and privacy protection strategies used in cloud computing with a comparative research study.

Keywords: *Cloud Computing, Data Security, Privacy, Protection, Security, Architecture, Consumers.*

I. INTRODUCTION

As the next generation paradigm of computation, cloud computing has been imagined. Both software and resources are distributed on demand over the Internet as services in the cloud computing world. Cloud is a data center hardware and software resource environment that provides different services over the network or the Internet to meet user requirements. Cloud computing can be called a modern archetype of computing that can deliver services at a low cost on demand [1]. Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service are the three well-known and widely used service models in the cloud paradigm (IaaS). In SaaS, software with related data is deployed by a provider of cloud services and can be used by users via web browsers. In PaaS, a service provider offers a collection of software programmes for consumers with services that can solve particular tasks [2]. The cloud service provider offers software for virtual machines and storage users in IaaS to expand their business capabilities [3].

Cloud computing can make it possible to readily access resources on demand. Cloud computing has features such as on-demand self-service, ubiquitous network connectivity, pooling of resources independently of venue, rapid resource elasticity, pricing based on usage, and risk transfer. Such benefits of cloud computing have drawn important interests from both the manufacturing sector and the world of academic science. Cloud computing technology is actually altering the world's way of doing business [4]. There has been a rapid advance in cloud computing over the past few years. Cloud Computing provides a broad range of technologies, such as processing power, Internet-based computing tools, storage and software for consumers. The Principal in the current segment of the industry, cloud providers are Amazon, Google, IBM, Microsoft, Salesforce, etc. With an increasing number of businesses resorting to using assets in there is a need for the cloud to secure the data of different users. Any big ones Cloud Computing faces the difficulties of safeguarding, securing and processing data which is the user's land. For IT applications, cloud computing is very promising; however, some problems remain to be solved for personal users and businesses to store data and deploy applications in the cloud computing world. Data protection, followed by concerns such as compliance, privacy, confidence, and legal matters, is one of the most critical obstacles to adoption [5].

A big concern in IT has consistently been data protection. In the cloud computing world, data protection is especially serious since data is distributed on numerous computers and storage devices, including servers, PCs, and various mobile devices, such as wireless sensor networks and smart phones [6]. In conventional information systems, data security in cloud computing is more complex than data security. The roles of cloud computing are first examined before the problems of data protection are addressed. Cloud computing is often referred to as a service on demand. There is a cloud service provider in the cloud computing world that facilitates applications and maintains the services. All services over the Internet are facilitated by the cloud provider, while end users use services to fulfil their business needs and then pay the service provider accordingly [7].

In this paper, in the cloud computing world, we will review various security strategies and challenges for data storage security and privacy protection. This paper provides a comparative research study of the latest research work on the techniques used in cloud computing across aspects of data protection, including data privacy, confidentiality, and availability. As data privacy is typically followed by data protection, data privacy issues and technology in the cloud are also studied. Comparative data protection and privacy studies may help to increase the trust of the user by protecting data in the cloud storage environment.

II. DISCUSSION

Data should not be lost by unauthorised users or changed by them. The foundation for the pro vision of cloud storage services such as SaaS, PaaS, and IaaS is data integrity. Cloud computi ng typically offers data processing services in addition to data storage of large scale data.

A. Data Integrity:-

In every information system, data integrity is one of the most important elements. Data integrity usually means shielding data from unauthorized deletion, alteration, or manufacturing. The admission and rights of the managing agency to unique business resources ensure that precious data and services are not misused, misappropriated or stolen. In a standalone system with a single database, data consistency is easily accomplished [8]. Data integrity is preserved in the standalone system by database restrictions and transactions, normally completed by a database management system (DBMS). To ensure data integrity, transactions should follow ACID (atomicity, accuracy, isolation, and durability) properties. Most databases allow transactions with ACID and can maintain the integrity of data.

B. Data Confidentiality:-

For users to store their private or confidential data in the cloud, data confidentiality is essential. To ensure data security, authentication and access control methods are used. In cloud computing, data protection, authentication and access control problems may be solved by increasing the security and trustworthiness of the cloud. Since users do not trust cloud providers and providers of cloud storage services are practically unable to remove possible insider attacks, it is very risky for users to directly store their confidential data in cloud storage. The key management issue is faced with simple encryption and does not support complicated requirements such as query, parallel alteration, and fine-grained permission [9].

C. Data Availability:-

The availability of data implies the following: when incidents such as hard disc destruction, IDC fire, and network failures occur, the degree to which user data can be used or retrieved and how users check their data through techniques rather than by the cloud service provider alone, depending on the credit guarantee. Customers are seriously worried about the storage of data on trans board servers because cloud providers are regulated by local laws, and so cloud customers should be aware of those laws. In addition, data protection, especially data confidentiality and integrity, should be guaranteed by the cloud service provider. In this connection, the cloud provider should share all such concerns with the client and establish a relationship of trust. The cloud provider can have data protection assurances and clarify the customers' authority over local laws. The key focus of the paper is on the data problems and challenges associated with the location of data storage and its relocation, cost, and security.

D. Data Privacy:-

Privacy is an individual or a group's ability to seclude themselves or information about themselves and thus selectively reveal them. Privacy has the elements that accompany.

1. When: A subject may be more worried about the disclosure of current or potential information than about past information.
2. How: If his or her friends can manually request his/her details, a user may be relaxed, but the user may not want notifications to be sent automatically and regularly.
3. Extent: instead of a particular point, a user may have his/her data reported as an undefined area.

III. CONCLUSION

Cloud computing for the next generation of IT applications is a promising and evolving technology. Data security and privacy problems are the barriers and obstacles to the exponential growth of cloud computing. A mandatory obligation of any organization is to reduce data storage and processing costs, while evaluating data and information is often the most critical activity for decision-making in all organizations. So, once confidence is established between cloud service providers and customers, no companies can move their data or information to the cloud. Researchers have suggested a range of strategies for data protection and to achieve the highest degree of data security in the cloud. However, by making these methods more successful, there are still many holes to be filled. In the field of cloud computing, further work is needed to make it relevant to the customers of cloud services.

IV. REFERENCES

[1] D. Chen and H. Zhao, “Data security and privacy protection issues in cloud computing,” 2012, doi: 10.1109/ICCSEE.2012.193.

[2] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications, 2013, doi: 10.1186/1869-0238-4-5.

[3] H. Takabi, J. B. D. Joshi, and G. J. Ahn, “Security and privacy challenges in cloud computing environments,” IEEE Security and Privacy, 2010, doi: 10.1109/MSP.2010.186.

[4] Z. Tari, “Security and Privacy in Cloud Computing,” IEEE Cloud Computing, 2014, doi: 10.1109/MCC.2014.20.

[5] W. Jansen and T. Grance, “Guidelines on security and privacy in public cloud computing?,” in Public Cloud Computing: Security and Privacy Guidelines, 2012.

[6] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, “Security and privacy in cloud computing: A survey,” 2010, doi: 10.1109/SKG.2010.19.

[7] Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Communications Surveys and Tutorials, 2013, doi: 10.1109/SURV.2012.060912.00182.

[8] B. Grobauer, T. Walloschek, and E. Stöcker, “Understanding cloud computing vulnerabilities,” IEEE Security and Privacy, 2011, doi: 10.1109/MSP.2010.115.

[9] L. M. Kaufman, “Data security in the world of cloud computing,” IEEE Security and Privacy, 2009, doi: 10.1109/MSP.2009.87.